Troubleshooting

De

Conectividade

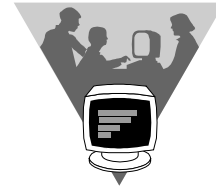
Em TCP/IP

Waldir C. Sola

Índice

Introdução ao Protocolo TCP/IP (IPv4)

TROUBLESHOOTING DE CONECTIVIDADE EM TCP/IP

Em 1957 o governo norte americano criou a ARPA (Advanced Research Projects Agency - Agência para projetos avançados de pesquisa) para encomendar e coordenar pesquisas às universidades para projetos de defesa do País, principalmente em função da guerra fria que existia naquela época, bastante latente.
.

Como a ARPA começou a crescer muito, começaram a surgir problemas de conectividade devido aos diferentes ambientes operacionais. Daí, em 1969 nasceu a ARPANET (Defense Advanced Research Projects Agency - DARPA), uma rede do Departamento de Defesa Norte Americano para pesquisas de protocolos de rede.

Criou-se o protocolo TCP/IP (Transmission Control Protocol/Internet Protocol - protocolo de controle de transmissão / protocolo entre redes) que foi desenhado para permitir multi plataformas se conectarem. Esta data , portanto, (1969) é considerada a data do surgimento da **Internet**.

O **TCP/IP** só se tornou padrão mundial de comunicação entre redes a partir de 1983. Desde então o objetivo da Internet era permitir que engenheiros e cientistas, que trabalhavam em projetos militares em toda a América do Norte, pudessem compartilhar computadores. Em 1984 foi estendido para órgãos de pesquisa e instituições educacionais.

No Brasil tudo começou em 1989, através do programa do Ministério da Ciência e Tecnologia, coordenado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico , que é a Rede Nacional de Pesquisa (RNP).

Em 1990, Tim Berners-Lee, do CERN (laboratório europeu para pesquisas relacionadas à física das partículas) desenvolveu um protocolo para transferência de diferentes tipos de arquivos através da Internet, usando um protocolo comum. Este foi o início do World Wide Web, ainda a caracter (ASCII). O NCSA (National Center for Supercomputing Applications, Illinois – USA) desenvolveu o MOSAIC, primeira front-end gráfica para a Internet.

O **WWW** representa o maior avanço da forma de acesso aos recursos da Internet. Totalmente gráfico, comandado por mouse, obtém-se informações de multimídia e todos os demais recursos da Internet de forma bastante amigável para qualquer usuário leigo.

Graças ao WWW a Internet passou a ser atrativa para todos e com isso o seu crescimento passou a ser geométrico. Antes, como acesso a caracter, se limitava a instituições científicas e educacionais.
Entretanto o uso comercial está cada vez mais acentuado.

Como esta forma de acesso se tornou muito popular, as empresas fabricantes de softwares rapidamente desenvolveram a idéia de se ter os recursos WWW dentro das empresas, transformando seus servidores de rede em servidores de Web, surgindo aí a Intranet.

O acesso a páginas de textos (HTML) é feito através de programas chamados de *Browsers*. O primeiro *browser* foi o Mosaic e atualmente os mais conhecidos são Netscape e o Internet Explorer da Microsoft.
Através de um *Browser* pode-se acessar telas WWW em hosts na Internet (ou Intranet) , fornecendo a URL (Uniform Resource Locator) além de FTP ,GOPHER, TELNET e outros serviços, desde que seu provedor tenha tais recursos instalados (ou, no caso da Intranet, tais recursos estejam instalados em seus servidores). Pode-se também fazer acesso a correio eletrônico (e-mail) e grupos de interesse (news group).
O último avanço da Internet é o advento do JAVA que altera a natureza passiva da Internet e da World Wide Web, permitindo que códigos de aplicações sejam executados em uma rede totalmente heterogênea de equipamentos, como é o caso da Internet, além da grande vantagem de sua codificação ser

otimizada, viabilizando o acesso mesmo em linhas de throughput baixo. O Java permite a criação de aplicações interativas complexas e a criação de imagens animadas e som.

A popularidade do protocolo TCP/IP se deu, de fato, com esta nova geração da forma de acesso aos recursos computacionais com o uso dos Browsers.

Ipv6

O problema de exaustão da capacidade de endereçamento previsto em Agosto de 1990 no meeting da IETF levou à criação, em Novembro de 1991, de um grupo de trabalho denominado ROAD (Routing and Addressing Group), que analisou e procurou soluções para este problema. O trabalho deste grupo,apresentado em Março de 1992, apontou essencialmente em duas direções:

- a curto prazo: desenvolver e aplicar políticas de atribuição de endereços que permitam atribuir várias classes C a organizações que necessitem de mais do que 256 endereços mas para as quais uma classe B seja excessiva
- utilizar agregações de redes de classe C de forma a evitar o anúncio de todas as redes diminuindo assim o crescimento das tabelas de roteamento.
- a longo prazo: desenvolvimento de um protocolo de rede que além de estender o espaço de endereçamento supere as limitações do IPv4 nomeadamente nos aspectos de: Encaminhamento de pacotes segundo políticas administrativas (policy-based routing);
- Controle de Fluxo;
- Qualidade de serviço “fraca”;
- Garantias de serviço (Qualidade de Serviço “Forte”);
- Contabilização.

A solução de curto prazo encontrada foi denominada de CIDR (Classless Inter-Domain Routing) e é mais um "balão de ar" do que propriamente uma solução, pois permite apenas adiar, por mais algum tempo, a data de exaustão do espaço de endereçamento que se prevê, atualmente, que seja para meados do ano 2010. O método CIDR consiste, essencialmente, na perda do valor semântico das classes de endereços passando a informação de roteamento a ser considerada em relação ao par (rede, máscara) ou (rede, n.º de bits significativos) em contraste com a situação original em que a máscara era obtida implicitamente por classe de endereçamento. A atribuição de endereços passa a ser feita de uma forma hierárquica por região ou provedor .

São reservados blocos de endereçamento para:

- Organizações multi-regionais;
- Europa (sob administração do RIPE);
- América do Norte;
- América Central e do Sul;
- Pacífico.

Subsequentemente, parte do espaço de endereçamento regional é atribuído a providers que operem dentro dessa zona geográfica.

Paralelamente foram desenvolvidos protocolos de routing inter-domínio e intra-domínio com capacidade para utilizar agregação de informação de routing segundo a norma CIDR.

IP, a geração seguinte

Em meados de 1992 a “Internet Authority Board” (IAB) publica um documento intitulado “IP version 7” onde preconiza “um esforço imediato por parte do IETF de forma a preparar um plano para a utilização futura de protocolo CLNP como a base para a versão 7 do protocolo IP”. O IETF decide não aceitar esta recomendação e emitir um pedido de propostas conforme o preconizado pelo grupo de trabalho ROAD.

Em resposta a este pedido formaram-se vários grupos de trabalho com vista ao estudo de possíveis sucessores do protocolo IP.

No meeting do IETF de Novembro de 1992 decorre uma sessão denominada “Selection Criteria BOF” com o objetivo de obter consenso em relação ao critério a aplicar na escolha do sucessor do protocolo

IPv4. Dos dois documentos preparatórios em discussão e dos pontos de vista expressos na reunião saiu um novo documento contendo os critérios de seleção tidos como consensuais.

Dispondo da sugestão do “Internet Engineering Steering Group” (IESG) em relação ao critério técnico a tomar na escolha do próximo protocolo IP delineada em RFC 1380 e dos resultados da discussão dentro do próprio IETF anteriormente referida, o IETF considera necessário um debate alargado sobre este tópico e emite um “call for white papers”. Em resposta a esta solicitação foram recebidos vinte e três artigos contendo os pontos de vista dos setores industrial, tecnológico e comercial.

Os documentos anteriormente referidos, os resultados da sessão “Next Generation Requirements” durante o encontro do IETF de Março de 1994 em Seattle e as discussões tidas na lista de mail “big-internet” foram utilizados por Frank Kastenholz e Craig Partridge para rever o seu “draft” inicial e produzir um documento intitulado “Technical Criteria for Choosing IP The Next Generation (IPng)”

Este documento propõe uma lista de objetivos e um conjunto de critérios a serem atingidos pelo protocolo IPng. Os objectivos enunciados, a nível geral, são os seguintes:

- Simplicidade de arquitetura.
- Um protocolo “comum” a todos os sistemas capaz de garantir a conectividade global.
- Longevidade.
- Aumento de funcionalidade em relação ao IPv4.
- Modelo cooperativo em termos de Internetworking.

A seguinte lista contem critérios específicos de avaliação recomendados, sendo a ordem irrelevante, as definindo o documento o tempo de disponibilização necessário para o item em questão.

- Escalabilidade (suporte para um mínimo de 1012 sistemas finais).
- Flexibilidade de topologias.
- Performance.
- Robustez.
- Estratégia de transição.
- Independência em relação ao meio físico.
- Serviço orientado a Datagrama sem garantia de entrega.
- Configuração, administração e operação.
- Segurança.
- Identificação única de um nó.
- Acessibilidade de especificações técnicas e algoritmos.
- Suporte de Multicast.
- Facilidades de extensão.
- Distinção do serviço oferecido pela rede (qualidade de serviço, reserva de recursos, etc.).
- Suporte de mobilidade.
- Protocolo de controle (funcionalidades de “debug”).

A 25 de Julho de 1994, é proposta uma recomendação do IPng no meeting da IETF em Toronto que é documentada no RFC 1752, sendo uma parte significativa do protocolo base proveniente do grupo de trabalho SIPP. Esta recomendação é aprovada a 17 de Novembro de 1994 e proposta como Standard. O conjunto base de protocolos do IPv6 é aprovado e proposto para Standard a 18 de Setembro de 1995.

Entretanto a ideia de criar uma rede de testes à semelhança da já existente para testes multicast (MBone) é posta em prática. Em Junho de 1996 concretiza-se esta ideia com a construção da rede 6Bone.

Características do IPv6 - IP next generation

O protocolo IPng foi desenhado como uma evolução do protocolo IPv4. As características do IPv4 que se consideram estar na base do sucesso do protocolo foram mantidas no IPv6. Funcionalidades que não tem um bom desempenho ou que são usadas raramente foram removidas ou tornadas opcionais.

Algumas novas capacidades que se consideram necessárias foram adicionadas sem, no entanto, alterar os conceitos base do IPv4.

As características mais importantes do IPv6 são:

- Extensão das capacidades de endereçamento e roteamento.

O tamanho de endereços passa de 32 bits na versão 4 para 128 bits no IPv6, o que permite o suporte de um número muito superior de nós finais, uma melhor hierarquização do espaço de endereçamento essencial à escalabilidade do roteamento e uma maior facilidade em termos de auto-configuração visto que permite a utilização de endereços IEEE-802 embutidos em endereços IPv6. A escalabilidade dos endereços multicast é também aumentada através da utilização de um campo que define o âmbito de alcance do datagrama. Os endereços podem ser unicast (globais, locais, link e de IPv4-compatíveis), multicast (one-to-many), de "cluster" (anycast: one-to-nearest) ou reservados.

Como curiosidade a capacidade total de endereçamento do novo protocolo é de 340.282.366.920.938.463.374.607.431.768.211.456 endereços, o que dá 665.570.793.348.866.943.898.599 endereços por m^2 do planeta Terra. No entanto, e tendo em conta as políticas de atribuição de endereços que possam vigorar, a visão mais pessimista prevê que venham a existir "apenas" 1564 endereços por m^2.

- Simplificação do cabeçalho

Alguns campos do cabeçalho IPv4 foram retirados ou passaram a ser opcionais de forma a simplificar o tratamento de um pacote comum. Embora os endereços IPv6 sejam 4 vezes maiores aos endereços IPv4 o cabeçalho é apenas duas vezes maior (40 bytes).

- Suporte para cabeçalho de extensão e de opções

As opções são codificadas, no IPv6, em cabeçalhos separados que se localizam entre o cabeçalho IPv6 e o cabeçalho de transporte. Visto que a maioria das opções apenas são examinadas e processadas por nós finais, esta codificação permite que a utilização de opções e extensões ao protocolo não interfira com a capacidade de encaminhamento de pacotes nos roteadores. Este suporte permite também que outras opções futuras possam ser incorporadas dando assim maior flexibilidade. Ao contrário do IPv4 onde o comprimento máximo da parte opcional do cabeçalho é de 40 bytes, o que se torna uma severa limitação à utilização de certas opções, as opções em IPv6 podem ser de comprimento arbitrário.

- Suporte para autenticação e privacidade

O protocolo IPv6 inclui as definições de extensões que permitem a autenticação e confidencialidade de comunicações ao nível de rede.

- Suporte de auto-configuração

A nova versão do protocolo possui mecanismos destinados a facilitar a gestão e configuração de ambientes IP através da utilização de mecanismos de auto-configuração. São definidos mecanismos de auto-configuração com manutenção de estado (dependentes de uma entidade que realiza a atribuição de endereços) e sem manutenção de estado. Esta funcionalidade é bastante útil para o estabelecimento de ligações móveis.

- Suporte para seleção de rota pelo originador

O IPv6 inclui uma extensão que permite a especificação de rota pelo originador desenhada para se integrar com a utilização do protocolo "Source Demand Routing Protocol" (SDRP). Este protocolo tem por

objetivo a seleção de rotas pelo originador de forma a completar o encaminhamento de pacotes com base na informação fornecida pelos protocolos de roteamento intra e inter-domínio correntes. Esta opção permite não só, controlar o tráfego na rede, como também aumentar a segurança na transmissão da informação.

- Transição simples e flexível

Uma das características chave do protocolo IPv6 é um plano de transição simples que permita a instalação incremental de nós IPv6 no ambiente atual. Este plano contempla a instalação de nós IPv6 sem exigir qualquer dependência em relação a outros nós e permitindo o endereçamento de nós IPv6 com base nos endereços IPv4 já atribuídos.

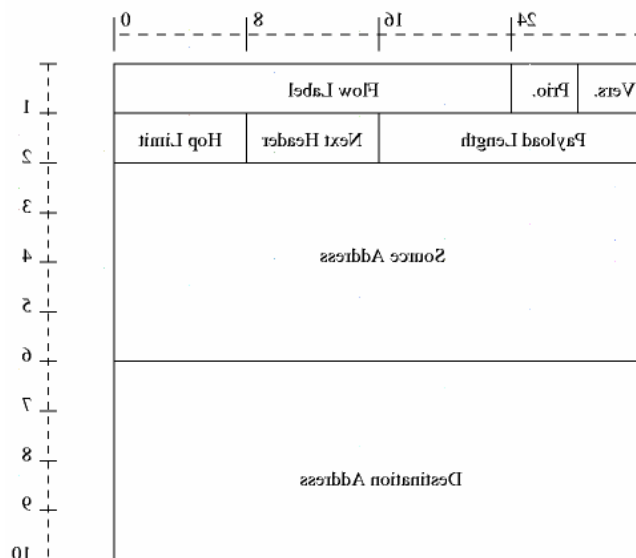
- Suporte para tráfego com garantia de qualidade de serviço

O cabeçalho IPv6 contem um campo de fluxo destinado a ser utilizado em conjunto com um protocolo de reserva de recursos de forma a permitir a utilização de qualidade de serviço garantida.

- Suporte para Jumbogramas

Possibilidade de enviar pacotes com dimensão superior a 64Kb. O limite de um pacote Jumbogram é de 4Gb (tamanho registado nos primeiros 32 bits do payload) sendo colocado o valor 0 no campo Payload Length do cabeçalho, indicando assim um Jumbogram. Esta propriedade é útil para as redes com grande largura de banda.

-Formato do Cabeçalho (Header)

Figura 1: IPv6 - Formato do cabeçalho

onde:

Version - Versão do protocolo (4 bits). Valor constante igual a 6.

Priority / Version Class - Indicador de prioridade (4 bits). Os valores de prioridade estão divididos em duas classes: valores de 0 a 7 são usados para especificar valores de prioridade de tráfego para o qual o originador providencia controle de congestionamento; os valores de 8 a 15 são utilizados para especificar a prioridade de tráfego para o qual não é realizado controlede congestionamento.

Flow Label - Identificador de fluxo (24 bits). Consiste num valor arbitrário que pode ser utilizado pelo originador para identificar pacotes para os quais tenha requerido uma determinada qualidade de serviço por meios externos ao protocolo IP em si. Um fluxo é uma sequência de pacotes enviados por um determinado originador a um destino específico para o qual o originador deseja um tratamento especial por parte dos roteadores intervenientes no encaminhamento de pacotes.
Payload Length - Número de bytes que seguem ao cabeçalho: tamanho do pacote seguinte (16 bits). Comprimento máximo 64 KB.
Next Header - Tipo do cabeçalho que se encontra imediatamente após o cabeçalho IPv6 (8bits).
Hop Limit - Número máximo de nós intermédios que o pacote pode percorrer. Este valor é decrementado de uma unidade em cada nó que encaminha o pacote (8 bits).
Source Address - Endereço de origem (128 bit).
Destination Address - Endereço de destino (128 bit).

A informação com relação às opções é codificada, no IPv6, em cabeçalhos separados que podem ser colocados entre o cabeçalho IPv6 e o cabeçalho do protocolo de transporte.

Vários cabeçalhos de extensão podem ser encadeados dado que cada opção é identificada por um valor distinto atribuído pela IANA.

À exceção de um cabeçalho de opção denominado "hop-by-hop", os cabeçalhos de extensão não são examinados ou processados por nenhum nó intermediário até o pacote ser entregue ao interface identificado pelo endereço de destino. O cabeçalho "hop-by-hop", quando presente, segue imediatamente o cabeçalho IPv6.

Os cabeçalhos são processados sequencialmente pelo destinatário. Ao encontrar um tipo de cabeçalho desconhecido, este deverá descartar o pacote e enviar uma mensagem de erro ao originador por ICMP - Internet Control Message Protocol.

Uma implementação completa de IPv6 inclui a implementação dos seguintes cabeçalhos de extensão:

- Opções nó-a-nó (Hop-by-Hop Options)
- Roteamento
- Fragmentação
- Opções de Destino
- Autenticação
- Privacidade (Encapsulating Security Payload)
- Endereçamento (addressing)
- Encaminhamento (routing)

O comprimento de um cabeçalho de extensão é múltiplo de 8 bytes de forma a manter o alinhamento de 8 bytes para os cabeçalho subsequentes.

Conceituação (IPv4)

Como já dito, o TCP/IP é um conjunto de protocolos para permitir a interconexão de ambientes heterogêneos em redes de computadores, ou seja, redes de diferentes topologias e hardwares de diferentes fabricantes e sistemas operacionais, os mais diversos, podem se comunicar através do TCP/IP.

O conjunto de protocolos TCP/IP define formatos e regras para a transmissão e recepção de informações independentemente de qualquer organização de rede ou hardware de computadores. Embora, a principio o TCP/IP tenha sido desenvolvido para a Internet, hoje é o padrão mundial de comunicação entre redes públicas e privadas no mundo, porque a Internet tornou-se mundial.

A rede de computadores, como concebida pela ARPANET e implementada com o conjunto de protocolos TCP/IP é uma rede de "troca de pacotes" (packet-switched).

Uma rede packet-switched transmite informações em pequenos segmentos, chamados de pacotes (packets). Se um computador transmitir um arquivo extenso para um outro computador, este arquivo será subdividido em pequenos segmentos na origem e reunidos no destino. Os protocolos TCP/IP definem o formato destes segmentos (pacotes).

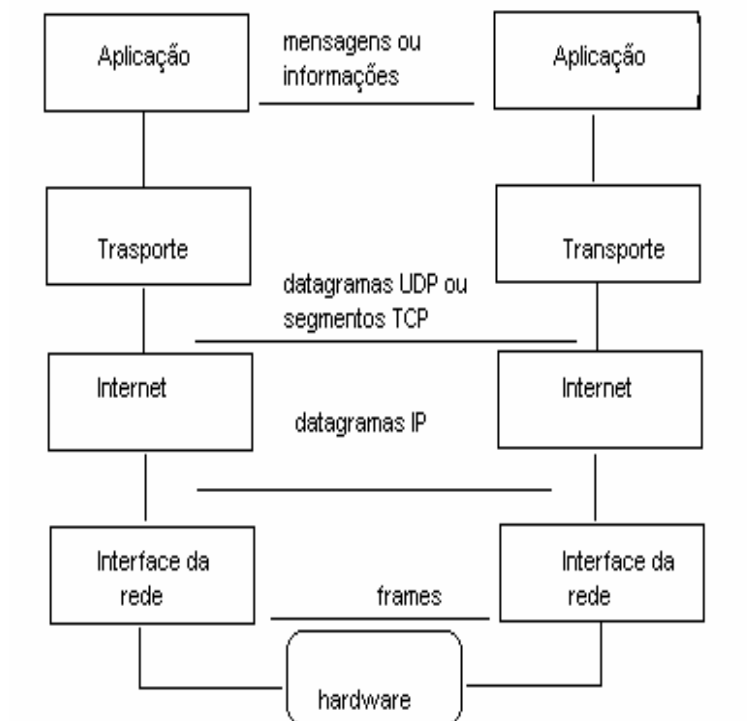
Esta definição também inclui o endereço origem e destino do pacote, o tamanho do pacote, o tipo do pacote e a forma como este pacote trafega na rede.

Os protocolos mais importantes do conjunto de protocolos do TCP/IP podem ser listados conforme tabela a seguir:

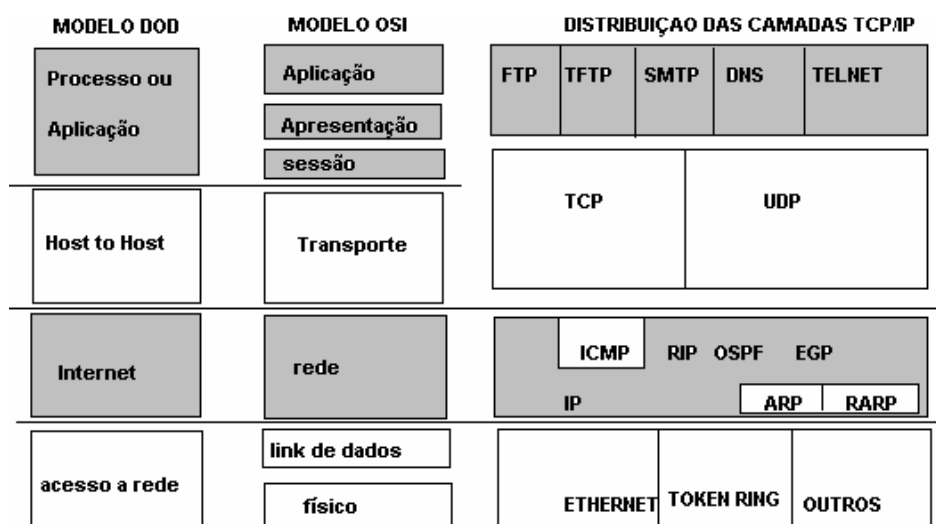
Protocolo		**Serviço**
IP	Internet Protocol	Provê o envio de pacotes entre nós (roteamento)
ICMP	Internet Control Message Protocol	Controla a transmissão de mensagens de erro e de controle entre hosts e gateways
POP3	Post Office Protocol version 3	Caixa Postal – recebimento de mensagnes
SMTP	Simple Mail Transfer Protocol	E-Mail – correio eletrônico – envio de mensagens
NFS	Network File System	Criado pela SUN, compartilhamento de volumes
SNMP	Simple NetWork Management Protocol	Protocolo de gerenciamento de rede
ARP	Address Resolution Protocol	Mapeia endereços Internet nos endereços físicos
RARP	Reverse Address Resolution Protocol	Mapeia endereços físicos em endereços Internet
TCP	Transmission Control Protocol	Envio de pacotes com controle de erro
UDP	User Datagrama Protocol	envio de datagramas clientes sem controle de erro.
LPD	Line Print Deamon	Impressão em linha
RPR	Remote Printing	Permite a impressão remota
TFTP	Trivial File Transfer Protocol	Serviços de transferência simplificada de arquivos.
FTP	File Transfer Protocol	Provê serviços de transferência de arquivos.
TELNET	Tele Networking	Provê emulação de terminal
X WIndow	Compartilhamento de aplicação	Permite a emulação gráfica de terminal UNIX
RIP	Routing Information Protocol	Permite a troca de informação de roteamento vetorial de distância entre roteadores
OPSF	Open Shortest Path First Protocol	Permite a troca de informação de roteamento de estado de link entre roteadores
DNS	Domain Name Server	Servidor de Nome de Domínio. Para permitir o acesso a hosts via nome ao invés do endereço IP
IGP	Interior Gateway Protocol	Usado para troca de informações de tabelas de roteamento entre roteadores vizinhos , na Internet. (RIP e OSPF são exemplos práticos de IGP.

IPCP	Internet Protocol Control Protocol	Um protocolo de controle de rede para protocolo ponto a ponto (PPP) que provê procedimentos para estabelecimento, configuração e termino da interação entre pontos em um link PPP.
EGP	Exterior Gateway Protocol	Permite a troca de informação de roteamento entre roteadores
BOOTP	Boot Protocol	Serviço de fornecimento automático de endereço IP para um HOST no momento de sua inicialização
DHCP	Dynamic Host Configuration Protocol	Serviço de fornecimento automático de endereço IP para um HOST no momento de sua conexão

Camadas do rede TCP/IP

Aplicações desenvolvidas para o TCP/IP, geralmente usam vários dos protocolos do conjunto de protocolos do TCP/IP.
A soma das camadas do conjunto de protocolos é chamada de pilha (stack).
A aplicação do usuário se comunica com a camada superior da pilha de protocolos.
A camada superior se comunica com a inferior que, por sua vez, se comunica com o hardware.
A camada física transfere a informação para o computador destino.
As camadas inferiores da pilha de protocolos do computador destino passam a informação para as camadas superiores que por sua vez passam para a aplicação.

Cada camada de protocolo dentro do conjunto de protocolos do TCP/IP desempenha várias funções, estas funções são independentes das outras camadas. Cada camada, entretanto, espera receber certos serviços da camada próxima inferior e cada camada provê certos serviços para a camada próxima superior.

Observe que, freqüentemente se usa o termo “camada” e há uma separação de atribuição entre as camadas. Na década de 70 o Departamento de Defesa dos Estados Unidos (DOD) procurou, pela primeira vez, definir um modelo de camadas de rede. Em seguida estabeleceu-se o Modelo OSI (Open System Interconnection) largamente utilizado por fabricantes de hardware e software na atualidade.

A figura a seguir, mostra a equivalente entre os modelos:

O objetivo do sistema de camadas é o de padronizar processos de desenvolvimento de softwares, onde o desenvolvedor de um produto para uma determinada camada só se preocupa com as regulamentações para a camada em desenvolvimento e com a troca de informações entre as camadas superior e inferior em estudo. Com isso o TCP/IP tornou-se realmente um padrão internacional de protocolo de comunicação viabilizando, portanto, uma rede mundial de computadores, como a Internet.

IP (Internet Protocol)

No conjunto de protocolos TCP/IP , todos os pacotes são enviados pelo serviço de envio de **datagrama** (datagrama delivery service) . O envio de datagrama não é garantido por este serviço.

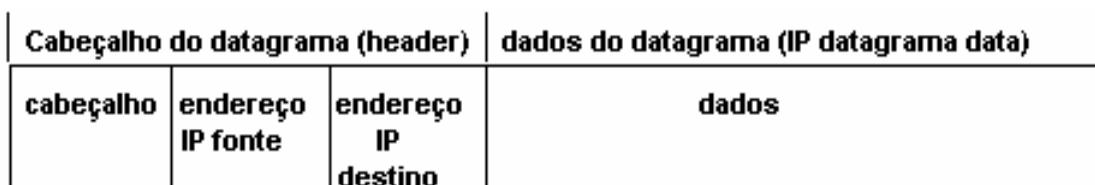
Um pacote pode ser enviado para o local errado, duplicado ou o perdido ao longo do caminho destino. O serviço não tem conexão de destino porque todos os pacotes são transmitidos independentemente de qualquer outro pacote. É diferente , por exemplo, da rede de telefonia, onde um circuito é estabelecido e mantido.

Os aplicativos em TCP/IP que utilizam o serviço de envio de datagramas IP mantêm o caminho do envio e esperam por uma resposta do nó de destino ou utilizam algum protocolo do conjunto de protocolos de transporte do conjunto de protocolos do TCP/IP.

O **IP** define a forma que os pacotes devem ter e a maneira como os pacotes devem ser manipulados quando os mesmos são transmitidos ou recebidos.

A forma que um pacote IP toma é chamada de **datagrama.** Um datagrama IP é análogo ao frame físico transmitido numa rede. Um datagrama contêm um cabeçalho (header) contendo um endereço IP do transmissor e do receptor, além de outras informações e os dados, efetivamente.

A seguir, um quadro esquemático do datagrama IP:

Cabeçalho do datagrama (header)			dados do datagrama (IP datagrama data)
cabeçalho	endereço IP fonte	endereço IP destino	dados

Quando um datagrama IP é enviado à rede , o mesmo é encapsulado no frame de dados da rede física, ou seja, é anexado ao frame físico.
Como o comprimento do frame físico é construído independentemente do datagrama IP devido exigências técnicas da placa de rede e da topologia da mesma, talvez um datagrama IP possa não caber dentro do frame físico.

Além disso, o datagrama IP pode trafegar em diferentes redes , com diferentes topologias, onde o tamanho dos frames físicos difere substancialmente.

Portanto, quando um roteador recebe um frame IP e o considera muito longo em relação à capacidade física de tamanho de frame da rede, este frame será subdividido em **fragmentos** (fragments) .

Estes fragmentos de datagrama IP serão montados quando encontrarem o destino final.

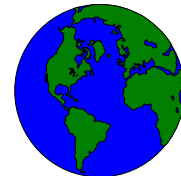
Endereçamento IP - Conceitos

Um endereço IP é necessário para que um nó se comunique com outros nós da rede , usando o conjunto de protocolos TCP/IP.

Cada nó da rede pode ser uma estação de trabalho, um servidor de rede, um roteador, um switch, uma impressora, ou seja, um equipamento de comunicação de dado sem TCP/IP deverá receber um endereço para que possa, efetivamente fazer parte da rede.,

Se sua rede não fizer parte da comunidade internacional, a Internet, você pode arbitrar um conjunto de endereços IP por sua conveniência.

No entanto, se você pretende fazer parte da Internet, o seu conjunto de endereços IP será fornecido, a princípio pela DDN Network Information Center - USA.

No caso do Brasil, será fornecido pela FAPESP.
Você pode consultar seu provedor mais próximo ou a EMBRATEL para proceder aos processos técnicos e administrativos para conexão de sua Intranet com a Internet.

Classes

Cada endereço IP é formado de 4 octetos (total de 32 bits), divididos em duas partes (Ipv4):

- uma porção para identificar o endereço de rede.
- uma porção para identificar o nó (chamado de host)

Os endereços IP são diferenciados em três classes baseadas nos 3 bits mais significativos dos quatro primeiros bits do endereço. Isto facilita aos roteadores identificar, facilmente, os endereços de rede. Os endereços IP são classificados por CLASSES.

As classes disponíveis são A, B e C:

O endereço de classe A consiste de uma porção de um byte de rede seguida de três bytes para host. O bit da maior ordem é zero. Podem, portanto haver 126 redes de classe A em uma rede interna (**1 a 126**), com mais de 16 milhões de nós, cada rede (0 e 127 são reservados)
(7 bits para endereço de rede e 24 para hosts)

O endereço de classe B consiste de uma porção de dois bytes de rede seguida de dois bytes para host. Os dois bits da maior ordem são 10. Podem, portanto haver quase 16.000 redes de classe B em uma rede interna (**128 a 191**), com mais de 65.000 nós, cada rede .
(14 bits para endereço de rede e 16 para hosts)

O endereço de classe C consiste de uma porção de três bytes de rede seguida de um byte para host. Os três bits da maior ordem são 110. Podem, portanto haver quase 2 milhões de redes de classe C em uma rede interna **(193 a 223**), com até 254 nós cada rede .
(21 bits para endereço de rede e 8 para hosts)

Em binário podemos observar em detalhes, no quadro abaixo:

Seleção da classe apropriada.

Ao decidir sobre qual classe de endereços IP utilizar em sua rede, deve-se levar em consideração o número de redes e o número de endereços de hosts necessários. No entanto para se conectar com a Internet, o conjunto disponibilizado de endereços IP será fornecido; portanto, você deverá ter que se adequar ao mesmo. Na necessidade de maior número de hosts, você pode utilizar o recurso da criação de sub-redes.

Endereços IP reservados.

Endereços de rede. Endereços IP onde a porção destinada aos hosts é igual a zero são endereços de rede. Por exemplo, o endereço 129.47.0.0 é um endereço de rede para uma rede da classe C.

Endereços de broadcast. São endereços onde a porção do host é igual a 1 (em binário). Um pacote com um endereço de broadcast é enviado para todos os nós da rede. Por exemplo, o endereço 129.47.255.255 é um endereço de broadcast para a rede 129.47.0.0

Endereços de loopack. O endereço de rede 127.0.0.0 e todos os endereços de hosts da rede, por exemplo, 127.0.0.1 são reservados. Geralmente utilizados para verificação da conexão lógica das camadas do protocolo TCP/IP.

Outros endereços reservados. Quando todos os bits forem zero ou todos os bits forem 1, são reservados para outras finalidades. Quando o IP for 0.0.0.0 implica em todas as redes. Quando for 255.255.255.255 indica broadcast de todas as redes. Segundo as RFC 1166 e 1918 há um conjunto de endereços com utilidades específicas. São eles:

ENDEREÇO	USO
10.X.X.X	REDES PRIVADAS
127.X.X.X	LOOPBACK
172.16.X.X A 172.31.X.X	REDES PRIVADAS
192.0.0.X	RESERVADO
192.0.1.X	BACKBONE PARA TESTE
192.0.2.X	BACKUP ONTERNET PARA TESTE
192.0.3.X A 192.0.255.X	NÃO ATRIBUIDO
192.1.0.X A 192.1.1.X	BACKBONE PARA REDE LOCAL
192.1.2.X	BACKBONE PARA REDES DE FIBRA ÓTICA
192.1.3.X	BACKBONE PARA REDES APOLLO
192.168.X.X	REDES PRIVADAS

Criação de sub-redes.

Uma rede Internet /Intranet pode ser subdividida em uma ou mais redes menores. Isto pode ser necessário nas seguintes situações:

- **Utilização de múltiplos meios de comunicação**: Pode ser impossível, inconveniente ou muito caro conectar todos os nós de uma rede quando estes nós forem muito distantes uns dos outros ou já estejam conectados a meios diferentes.

- **Redução de congestionamento**: os nós de uma rede única utilizam a mesma banda passante para o tráfego de dados. À medida que o número de nós vai aumentando, haveria a necessidade de se aumentar a banda passante para não ocorrer perda de desempenho na rede. Isolando os nós em redes separadas reduz o número de nós por rede, reduzindo, como conseqüência, o congestionamento da rede.

- **Redução do uso da CPU**: em uma rede mais segmentada, cada host tem menos trabalho em tratar os broadcasts naturais da rede, melhorando o desempenho de cada nó e de toda a rede.

- **Isolar a rede**: não só melhora o desempenho como também facilita o gerenciamento da rede, já que falhas em nós serão tratadas em cada segmento da rede.

- **Melhorar a segurança**: Dados sensíveis que passam por um segmento de rede não poderão ser monitorados em outros segmentos, melhorando a segurança dos dados.

- **Utilização racional de endereços IP**: Quando você recebe endereços IP de rede, você está limitado ao número possível de nós, em função da classe de endereços à sua disposição. Você pode subdividir esta rede em sub-redes para obter mais disponibilidade de nós sem ter que solicitar mais endereços para uso em sua rede.

Endereços de sub-rede e máscaras.

endereço de rede	porção do host
<network>	<subnetwork><host addr>

Cada sub-rede funciona como se fosse uma rede independente Quando uma rede é dividida em sub-redes, a porção de endereço de host do endereço IP é dividida em duas partes, exatamente como se o endereço IP fosse dividido em duas partes. A porção de endereço de host especifica tanto o endereço da sub-rede como o endereço de host na sub-rede.

Exemplo:

O endereço de rede **129.47.0.0** é da classe B, permitindo 65.534 endereços de hosts (pois os dois últimos bytes são usados para especificar endereços dos hosts). Nesta forma a máscara da sub-rede será **255.255.0.0**. Os dois últimos bytes para hosts totalizam 16 bits. Vamos pegar 4 bits iniciais do primeiro byte de host para que o mesmo seja utilizado para sub-rede. Restarão, portanto, 12 bits para hosts.

Portanto, para a rede **129.47.0.0**, a nova máscara de rede será **255.255.240.0** permitindo a criação de 15 novas sub-redes, cada uma comportando 4094 hosts (total de hosts nas sub-redes = 61.410 hosts)

rede	129	47	0	0
binário	1000 0001	0010 1111	0000 0000	0000 0000
mascara	255	255	0	0
rede	129	47	0	0
mascara	255	255	240	0
binário	1111 1111	1111 1111	1111 0000	0000 0000

Fisicamente as sub-redes são isoladas, e a interligação entre as mesmas é feita por **roteador**. O roteador pode ser um equipamento dedicado para isto (CISCO, 3COM, DIGITEL, IBM, etc.) ou mesmo um servidor de rede (Novell, NT, Unix, Main-Frame, etc.) com duas ou mais placas de rede ou mais, onde cada placa comportará um único segmento de rede.

Por exemplo:

Vamos dividir a rede 129.47.0.0 em duas sub-redes conforme a máscara 255.255.240.0. Criaremos as sub-rede 129.47.128.0 e a sub-rede 129.47.192.0

rede	129	47	128	0
binário	1000 0001	0010 1111	1000 0000	0000 0000
mascara	1111 1111	1111 1111	1111 0000	0000 0000
rede	129	47	192	0
binário	1000 0001	0010 1111	1100 0000	0000 0000
mascara	1111 1111	1111 1111	1111 0000	0000 0000

Para cada uma das redes, os endereços IP possíveis serão:

rede	129	47	128	0	
binário	1000 0001	0010 1111	1000 0000	0000 0000	
mascara	1111 1111	1111 1111	1111 0000	0000 0000	
menor	1000 0001	0010 1111	1000 0000	0000 0001	129.47.128.1
maior	1000 0001	0010 1111	1000 1111	1111 1110	129.47.143.254

rede	129	47	**192**	0	
binário	1000 0001	0010 1111	**1100** 0000	0000 0000	
mascara	1111 1111	1111 1111	1111 0000	0000 0000	
menor	1000 0001	0010 1111	**1100** 0000	0000 0001	129.47.**192**.1
maior	1000 0001	0010 1111	**1100** 1111	1111 1110	129.47.**207**.254

Para a rede 129.47.0.0 as sub-redes possíveis são as seguintes:

Subnet Address List

Selected Rows and Columns to Clipboard

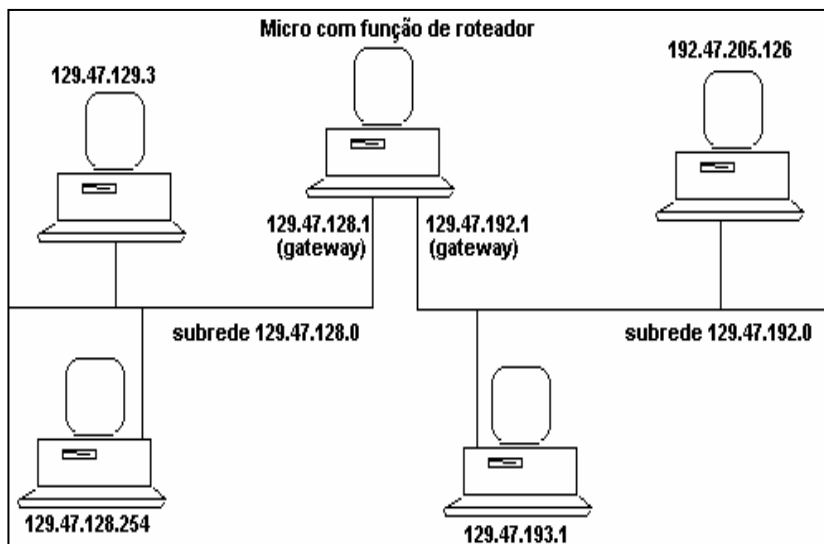
☑ Number ☑ Subnet Address ☑ Broadcast Address ☑ Address Range [Copy]

1	129.47.16.0	129.47.31.255	129.47.16.1 to 129.47.31.254
2	129.47.32.0	129.47.47.255	129.47.32.1 to 129.47.47.254
3	129.47.48.0	129.47.63.255	129.47.48.1 to 129.47.63.254
4	129.47.64.0	129.47.79.255	129.47.64.1 to 129.47.79.254
5	129.47.80.0	129.47.95.255	129.47.80.1 to 129.47.95.254
6	129.47.96.0	129.47.111.255	129.47.96.1 to 129.47.111.254
7	129.47.112.0	129.47.127.255	129.47.112.1 to 129.47.127.254
8	129.47.128.0	129.47.143.255	129.47.128.1 to 129.47.143.254
9	129.47.144.0	129.47.159.255	129.47.144.1 to 129.47.159.254
10	129.47.160.0	129.47.175.255	129.47.160.1 to 129.47.175.254
11	129.47.176.0	129.47.191.255	129.47.176.1 to 129.47.191.254
12	129.47.192.0	129.47.207.255	129.47.192.1 to 129.47.207.254
13	129.47.208.0	129.47.223.255	129.47.208.1 to 129.47.223.254
14	129.47.224.0	129.47.239.255	129.47.224.1 to 129.47.239.254

[Print All Rows...] [Close]

A seguir os cálculos binários para o host 129.47.128.1 pelo shareware **Subnet Calculator**

A seguir os cálculos binários para o host 129.47.143,254 pelo shareware **Subnet Calculator**

Temos, esquematicamente, as duas sub-redes separadas por um roteador:

Sub-redes de tamanho variável.

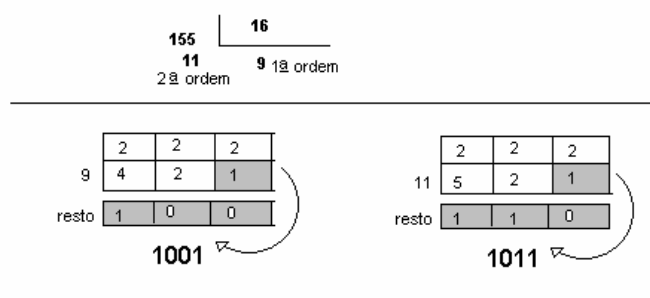
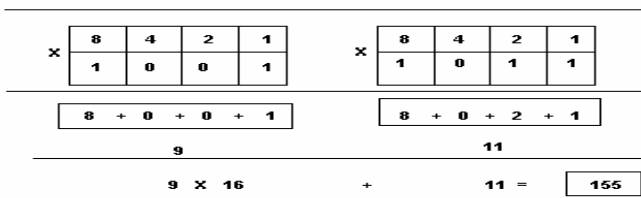
Uma sub-rede de uma rede pode ser subdividida em unidades de sub-rede menores. Estas sub-redes são chamadas de sub-redes de tamanho variável (variable size subnetworks). São chamadas de variáveis porque o tamanho da sub-rede varia de sub-rede para sub-rede. Quando o comprimento da máscara de sub-rede aumenta, o tamanho da sub-rede diminui, já que o endereço IP tem tamanho fixo de 32 bytes.

Uma máscara de sub-rede define o número de bits que podem ser usados para sub-rede e o número de hosts. Quando a máscara aumenta o número de hosts diminui. Quando a máscara diminui o número de hosts aumenta.

Algumas redes tem sub-redes com grande número de hosts e outras sub-redes tem pequeno número de hosts. Ao se utilizar a mesma máscara de sub-rede para todas as sub-redes pode levar às seguintes conseqüências:

- a máscara é muito pequena e você não tem número suficiente para criar todas as sub-redes.
- A máscara é muito grande e você não tem números IP's para todos os hosts da sub-rede.

Se a máscara não atende às suas necessidades, utilize a sub-rede de tamanho variável. Variando a máscara da sub-rede usada na rede, pode-se adequar ao número necessário de sub-redes e hosts.

Um método prático para conversão decimal / binário:

Um método prático para conversão binário /decimal :

EXERCÍCIOS

- Você precisa criar uma rede IP e o endereço de rede que lhe é oferecido é **132.7.0.0**. Com este endereço você precisa montar **5 sub-redes** com **1500 estações** de trabalho por sub-rede.

  Compute as seguintes informações na ordem solicitada:

  1. encontre o número de bits de host que você precisa pegar do octeto para conseguir o número de sub-redes necessário.
  2. Calcule o número de hosts por sub-rede que você conseguirá.
  3. Calcule , em decimal, a máscara de sub-rede que deverá ser usada.
  4. Informe, para cada sub-rede conseguida, qual o endereço do primeiro e do último host e qual o endereço de broadcast.

- Os micros com os respectivos endereços **192.168.2.9** e **192.168.2.20** , ambos com a máscara **255.255.255.248** estão em um mesmo segmento de rede. Como está a comnicação entre eles ?

Protocolos TCP/IP na camada de Aplicação.

Telnet.

Um microcomputador em uma rede IP pode acessar um main-frame ou um super-micro UNIX através do Telnet. Esta aplicação permite a "emulação" de terminal, ou seja, o micro funciona como um terminal do main-frame ou super-micro, a carcter (ASCII).

Em geral a solicitação de emulação do terminal dá-se pelo comando TELNET <endereço_IP> do servidor ou <nome-do-DNS-do-servidor>.

Só se consegue emular um terminal, via Telnet em um servidor que tenha disponibilizado este serviço. A disponibilidade do serviço é feita via um programa que roda no servidor, que permite o acesso remoto. Este programa se chama "deamon" .

Na Internet pode-se emular terminais da rede mundial que tenham o serviço de Telnet disponibilizado. No seu Browser digite: telnet://<nome_do_host_remoto> ou telnet://<endereço_ip_do_host_remoto>.

FTP

O FTP (File Transfer Protocol) permite a transferência de arquivos entre seu microcomputador e um host remoto. Em uma rede local, permite a troca de dados entre microcomputadores. Também, como no caso do Telnet, o Host que receberá uma solicitação de conexão, via FTP, deverá ter um "deamon" ativo, que permita o acesso remoto.

O FTP é feito via o comando FTP <nome_do_host_remoto> ou FTP <endereço_IP_do_host_remoto.

Na Internet pode-se acessar hosts remotos via FTP através do comando:
ftp://<nome_do_host_remoto ou ftp://<endereço_IP_do_host_remoto.

Em geral, dependendo da configuração do FTP do host remoto, lhe será solicitado um username e um password. Após a conexão estabelecida, uma série de comandos poderá ser executada para transferência bidirecional de arquivos.

A seguir , alguns dos comandos mais comuns do FTP:

Comando	Descrição do comando
?	Lista todos os comandos disponíveis
!	Vai para o DOS na estação local. Tecle EXIT para retornar ao FTP
open	Estabelece uma sessão FTP com um host remoto
close	Finaliza uma conexão FTP e mantêm o prompt do FTP ativo
quit	Encerra uma sessão FTP
get	Copia um arquivo remoto para o diretório corrente na estação local
put	Copia um arquivo local para um diretório da estação remota
help	Mostra as informações de ajuda dos comandos disponíveis
cd	Muda de diretório na estação remota
lcd	Muda de diretório na estação local
dir	Lista o conteúdo do diretório remoto corrente
ldir	Lista o conteúdo do diretório local corrente
mget	Copia múltiplos arquivos da estação remota para a estação local no diretório corrente
mput	Copia múltiplos arquivos da estação local para a estação remota no diretório corrente
Ascii	Configura o modo de transferência de arquivos para ASCII
binary	Configura o modo de transferência de arquivos para binário
Prompt	Alterna o prompt interativo para transferências de múltiplos arquivos
Exec	Executa um comando específico no host remoto
Pwd	Mostra qual o subdiretório corrente na estação remota

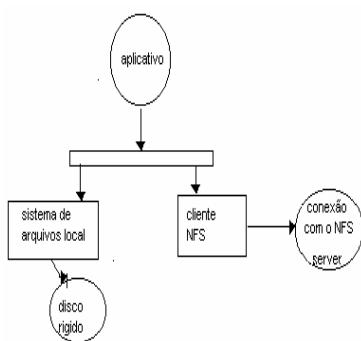
No quadro abaixo, hard copy do help to FTP:

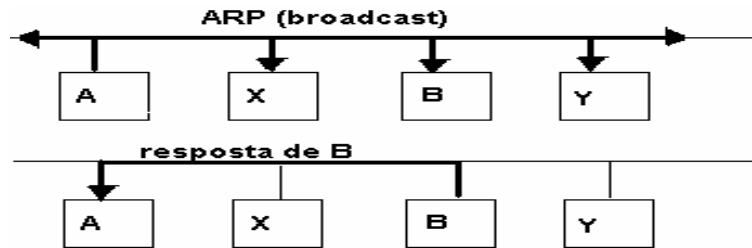
```
C:\WIN95>ftp
ftp> help
Commands may be abbreviated.  Commands are:

!          delete       literal    prompt     send
?          debug        ls         put        status
append     dir          mdelete    pwd        trace
ascii      disconnect   mdir       quit       type
bell       get          mget       quote      user
binary     glob         mkdir      recv       verbose
bye        hash         mls        remote     help
cd         help         mput       rename
close      lcd          open       rmdir
ftp>
```

TFTP

Trivial File Transfer Protocol (TFTP) é uma alternativa bastante simplificada para usuários não muito experientes em computação. Além disso, o TFTP se restringe à operação de transferência de arquivo sem as funções mais sofisticadas do FTP, embora permita a transferência de múltiplos arquivos.Muito utilizado no download de programas de atualização de flash-eprom de roteadores, impressoras de rede, e BIOS de computadores.

NFS

O NFS (Network File System), desenvolvido pela Sun Microsystems Incorporated, provê acesso compartilhado on-line a arquivos de forma transparente e integrada. Muitos sites TCP/IP usam o NFS para interconectar os sistemas de arquivos de seus computadores. Do ponto de vista do usuário , o NFS é quase invisível. O usuário pode executar um programa e usar arquivos para entrada e saída de dados. Os nomes de arquivos, por si só, não mostram se os arquivos são locais ou remotos.
Quando um programa executa, ele chama o sistema operacional para abrir um arquivo ou armazenar e recuperar dados de arquivos. O mecanismo de acesso aceita a solicitação e passa-a de forma automática ou para o sistema de arquivos local ou para o cliente NFS, dependendo de ou o arquivo estar em um driver local ou remoto. Quando ele recebe um pedido, o software NFS do cliente usa o protocolo para contatar o servidor apropriado em uma máquina remota e executa a operação solicitada. Quando o servidor remoto responde, o software cliente retorna o resultado ao aplicativo.

ARP

Duas máquinas, em uma rede física, só podem se comunicar se uma souber o endereço físico da outra. Suponhamos duas máquinas A e B que compartilham uma rede física. Cada uma tem um endereço IP, I_a e I_b e seus respectivos endereços físicos F_a e F_b. O objetivo é garantir que o software de mais baixo nível se comunique através de seus endereços físicos e permita que os programas de maior nível trabalhem somente com endereços IP. No entanto, a comunicação ocorre , de fato, sobre as redes físicas, utilizando os endereços físicos das placas de rede.

Suponha que a máquina A queira enviar um pacote para a máquina B, através da rede física, à qual ambas estão conectadas, mas A só sabe o endereço IP da máquina B. Como então que a máquina A vai saber qual o endereço físico (placa de rede) da máquina B ?

A solução está no *ARP*, Address Resolution Protocol (Protocolo de identificação de Endereço).

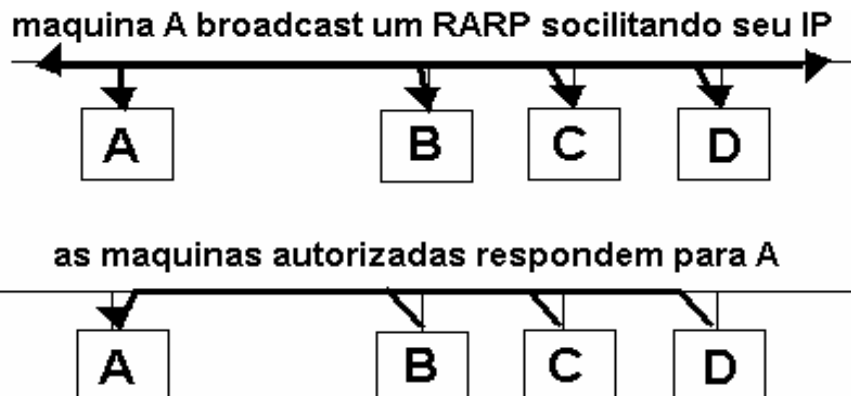
Quando A quer identificar o endereço físico de B, ele envia um broadcast de um pacote especial que pergunta a todos os hosts da rede, qual o endereço físico. No entanto, somente o host B, que tem o endereço IP identificado no pacote, responderá ao broadcast. Assim, A saberá qual o endereço físico de B.

A seguir apresentamos o datagrama ARP:

HARDWARE TYPE		PROTOCOL TYPE
HLEN	PLEN	OPERATION
SENDER HA (OCTETOS 0-3)		
SENDER HA (4-5)		SENDER IP (0-1)
SENDER IP (2-3)		TARGET HA (0-1)
TARGET HA (2-5)		
TARGET IP (0-3)		

HARDWARE TYPE especifica um tipo de interface de hardware para o qual quem envia (sender) procura por uma resposta. Contêm o valor 1 para Ethernet.
PROTOCOL TYPE especifica o tipo de protocolo. Contêm o valor 0800 para IP.
OPERATION valoe 1 para solicitação de endereço (request) e 2 para resposta (response).
HLEN especifica o comprimento do endereço de hardware e *PLEN* o comprimento do endereço de alto nível.

Quando o datagrama está fazendo um request, o sender também fornece o endereço IP destino (target), no caso do ARP ou o endereço de hardware destino (RARP), usando os campos TARGET HA ou TARGET IP, respectivamente.

RARP

Reverse Address Resolution Protocol é a situação inversa. Um host precisa conhecer seu endereço IP. Em geral, uma estação diskless, envia um pacote RARP, que tem o mesmo lay-out do ARP, fornecendo seu endereço físico (MAC), solicitando seu endereço IP. Um servidor de RARP que tenha a informação, responderá e colocará o endereço IP do host solicitante no campo TARGET IP.

BOOTP (BOOTstrap Protocol)

O BOOTP é uma alternativa para o RARP em estações diskless e atende, também, a estações com disco, para a determinação do endereço IP. O BOOTP é mais geral que o RARP porque utiliza UDP, possibilitando estender o bootstrap através de um gateway, ou seja, o RARP só funciona dentro de um único segmento de rede. Também permite que uma máquina determine um endereço de gateway, um endereço de um servidor de arquivos e uma máscara de sub-rede. Permite que administradores de rede estabeleçam uma base de dados que mapeie um nome genérico, como *unix*, dentro de um nome de arquivo determinado que contenha uma imagem de memória apropriada para o hardware cliente.

O BOOTP é projetado para ser pequeno e simples suficientemente para residir em um ROM de bootstrap. O cliente utiliza o endereço limitado de broadcast para se comunicar com o servidor, e toma a responsabilidade de retransmitir as solicitações se o servidor não responder.

Para se ter uma implementação tão simples quanto possível, as mensagens do BOOTP tem campos de comprimento fixo e as respostas tem o mesmo formato das solicitações.

As máquinas que enviam uma solicitação de BOOTP são as Clientes e as que respondem a uma solicitação de BOOTP são as servidoras.

A seguir, é apresentado o formato da mensagem de BOOTP:

FORMATO DAS MENSAGENS DE BOOTP

OP	HTYPE	HLEN	HOPS
TRANSACTION ID			
SECONDS		NÃO USADO	
CLIENT IP ADDRESS			
YOUR IP ADDRESS			
SERVER IP ADDRESS			
GATEWAY IP ADDRESS			
CLIENT HARDWARE ADDRESS (16 OCTETOS)			
SERVER HOST NAME (64 OCTETOS)			
BOOT FILE NAME (128 OCTETOS)			
VENDOR-SPECIFIC AREA (64 OCTETOS)			

OP: especifica se a mensagem é uma solicitação (1) ou uma resposta (2).

HTYPE: Tipo do hardware de rede (como no ARP) – Ex.: Ethernet é do tipo 1.

HLEN: Comprimento do endereço físico (Para o Ethernet = 6)

HOPS: O Cliente coloca zero neste campo. Se um servidor receber a solicitação e decidir passar adiante, o campo será incrementado em 1.

TRANSACTION ID:
Contém um inteiro que máquinas diskless utilizam para compatibilizar respostas com solicitações.

SECONDS: Reporta o número de segundos que passaram desde que o cliente iniciou seu boot.

CLIENT IP ADDRESS:
Se o cliente não sabe seu endereço, ele é preenchido com zeros. O cliente pode saber

seu endereço e apenas querer do servidor o BOOT FILE NAME para o boot.

YOUR IP ADDRESS:

Quando o cliente não sabe seu IP, o servidor coloca o endereço do cliente neste campo.

SERVER IP ADDRESS:

Se a estação souber qual o endereço IP do servidor de BOOTP ou o respectivo SERVER HOST NAME, então estes campos serão preenchidos com a informação e Somente o servidor especificado irá responder à solicitação. Se estes campos estiverem Vazios, todos os servidores BOOTP irão responder.

GATEWAY IP ADDRESS:

Quando houver, o servidor de BOOPT informa o gateway neste campo.

CLIENT HARDWARE ADDRESS:

Será informado pelo Cliente se o BOOTP estiver configurado para endereços fixos.

SERVER HOST NAME

O cliente informa o nome do servidor se souber, neste caso, só ele irá responder ao pedido.

BOOT FILE NAME:

Nome do arquivo imagem da estação cliente diskless.

VENDOR-SPECIFIC AREA:

Contém informações opcionais a serem passadas do servidor ao cliente. Os primeiros quatro octetos do campo são chamados de *magic cookie* e definem o formato dos itens restantes. São informações do tipo, máscara de sub-rede, gateways adicionais, hora do servidor, hora do dia, IP do servidor de domínio, servidores de impressão, etc.

DHCP (Dynamic Host Configuration Protocol)

Tem a mesma função do Bootp, adicionando-se a capacidade de alocação dinâmica de endereços de rede reutilizáveis e opções adicionais de configuração. Foi idealizado por R. Droms, da Bucknell University, em outubro de 1993, através do RFC 1531. O DHCP foi idealizado no modelo cliente/servidor, onde os hosts servidores de DHCP alocam endereços de rede e enviam parâmetros de configuração a hosts configurados dinamicamente. O DHCP suporta três mecanismos para alocação de endereços IP:

Alocação automática. O DHCP atribui um endereço IP permanente a um Host.

Alocação dinâmica. O DHCP atribui um endereço IP a um host por um período limitado de tempo (ou até que o host explicitamente descarte o endereço - leasing).

Alocação manual. O endereço do host é atribuído manualmente pelo administrador da rede.

O formato das mensagens DHCP é exatamente igual ao formato das mensagens do BOOTP e são totalmente interoperáveis, com exceção do campo VENDOR SPE CIFC AREA de 64 octetos que foi substituído por um campo de opções com tamanho mínimo de 312 octetos (tamanho máximo da mensagem do DHCP é de 576 octetos).

Interação cliente servidor – alocação de um endereço de rede:

1. O cliente envia um broadcast para a sua subrede física de uma mensagem DHCPDISCOVER.
2. Cada servidor pode responder com uma mensagem DHCPOFFER, oferecendo um endereço.
3. O cliente recebe as mensagens DHCPOFFER escolhe um servidor e envia um DHCPREQUEST
4. O servidor selecionado envia um DHCPACK contendo os parâmetros necessários para o host
5. Caso não seja capaz de atender a solicitação, envia um DHCPNAK.

Portas de Comunicação (Ports)

Cada serviço Internet, do conjunto de protocolos do TCP/IP tem identificado um número. Este número especifica o serviço que está sendo executado ou a conexão estabelecida. Por exemplo, a porta 21 está reservada para serviços de FTP enquanto a porta 23 está reservada para o serviço de TELNET.

O intervalo válido de portas vai de 1 a 65.535, distribuidos da seguinte forma:

- ✓ Portas bem conhecidas (Well Known Ports): de 0 a 1.023.
- ✓ Portas registradas: de 1.024 a 49.151
- ✓ Portas Dinamicas e/ou Privadas: de 49152 a 65.535

Veja alguns exemplos a seguir:

PORTA	UDP	TCP	SERVIÇO
1		X	TCPMULX – MULTIPLEXAÇÃO
5		X	RJE- REMOTE JOB ENTRY
7	X	X	ECHO
9	X	X	DISCARD
11	X	X	SYSTAT – ACTIVE USERS
13	X	X	DAYTIME
15	X	X	NETSTAT (NETOWRK STATUS)
17	X	X	QOTD (QUOTE OF THE DAY)
19	X	X	CHARGEN-CHARACTER GENERATOR
20		X	FTP-DATA – Dados na transmissão via FTP
21		X	FTP
23		X	TELNET
25		X	SMTP – Simple Message Transfer Protocol
37	X	X	TIME
67	X		BOOTPS-Bootpstrap Protocol Server
68	X		BOOTPC- Bootstrap Protocol Client
69	X		TFTP – Trivial File Transfer Protocol

Solução de problemas de Conectividade:

Sintomas:

Não consigo me comunicar com uma estação cliente Windows.
Não consigo dar *ping* em uma estação cliente Windows.
Não consigo resolver nomes DNS com uma estação cliente Windows.
Não consigo me logar a um servidor de rede.

Solução: Usar as dicas oferecidas pelas ferramentas do Windows.

==

Troubleshooting TCPIP a partir de um cliente Windows 95/98 client e Windows NT .

==

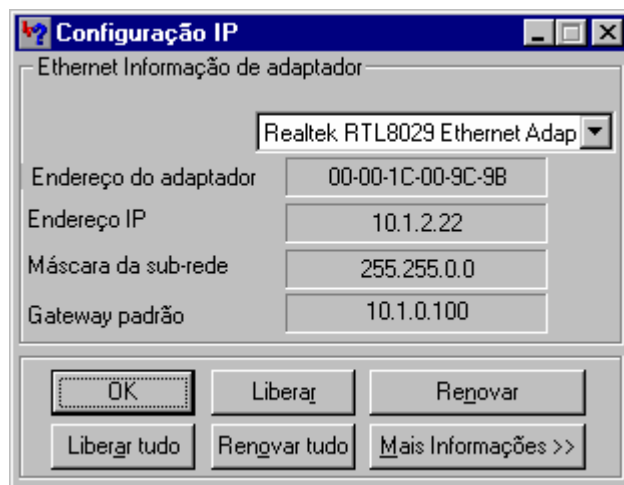
A pilha operacional do Windows 95/98 TCPIP e Windows NT 4.0 vem com alguns utilitários que estão disponíveis para qualquer usuário para ajudá-lo a determinar se o TCP/IP está funcionando e ajudá-lo a apontar onde podem estar ocorrendo problemas na rede.

==**1A.**

WINIPCFG – disponível no Windows 95/98

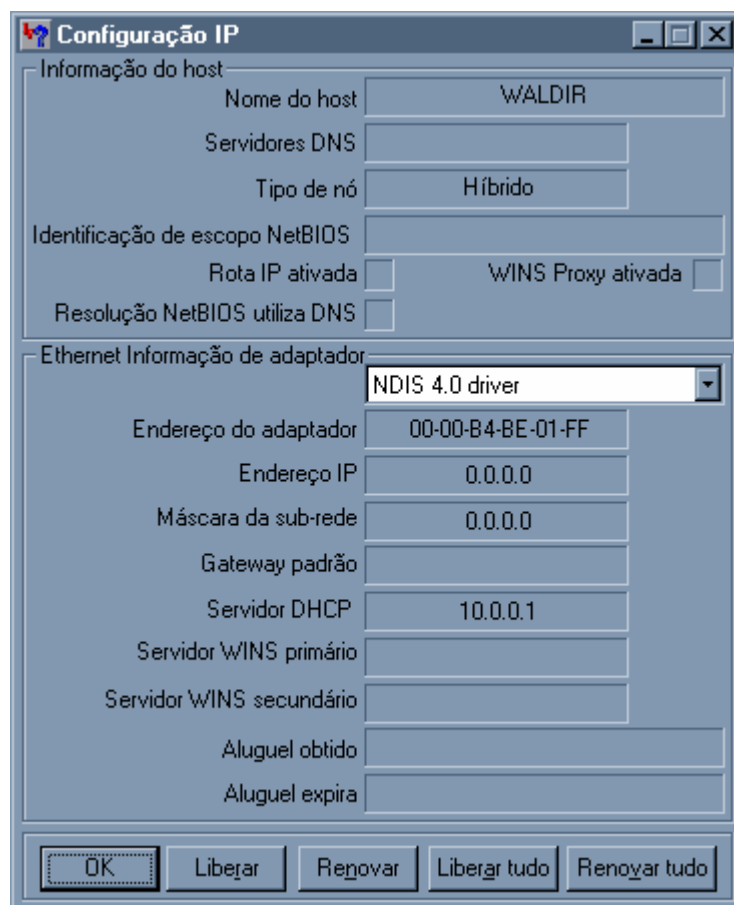
==

Winipcfg.exe é um utilitário que irá mostrar a configuração corrente TCP/IP da estação cliente. O comando pode ser executado clicando em INICIAR/EXECUTAR e entrando com a string WINIPCFG. Se o endereço IP foi colocado manualmente, as informações mostradas serão aquelas introduzidas na regulagem de rede pelo Painel de Controle. Se a estação obtiver o endereço através de um servidor de DHCP as informações mostradas serão aquelas fornecidas pelo servidor de DHCP.

Winipcfg oferece as seguintes informações:

Se a estação obtiver o endereço através de um servidor de DHCP, clicando **em Mais Informações >>** será mostrado o endereço do servidor de DHCP, quando o leasing começou e quando o leasing irá expirar. Além disso 4 outros botões estarão disponíveis: **Renovar**, **Liberar**, **Renovar tudo** e **Liberar tudo**.
Pressionando **Renovar** fará com que a estação cliente envie um **DHCPREQUEST** para o servidor de DHCP e atualizar o leasing e demais informações que são atribuídas pelo servidor de DHCP, como, por exemplo, o gateway padrão ou o servidor de DNS.

Selecionando **Liberar** fará com que a estação envie um pacote de **DHCPRELEASE** ao servidor de DHCP , significando que a estação está abandonando o endereço IP atribuído e permitindo que o servidor de DHCP ofereça o mesmo endereço a outra estação.
Se você quiser um outro endereço IP atribuído você deve selecionar **Renovar** logo após ter selecionado **Liberar**.
Renovar tudo e **Liberar tudo** são usados quando a estação tem mais de um adaptador de rede e você quer que as ações sejam executadas em todos os adaptadores simultaneamente.

O comando pode ser executado via prompt do DOS, ou seja, **WINIPCFG RENOVAR** ou **WINIPCFG LIBERAR** para realizar as mesmas funções.

Se você tiver a versão em inglês os botões são :RENEW, RENEW ALL, RELEASE, RELEASE ALL para, respectivamente, Renovar, Renovar tudo, Liberar e Liberar tudo.

===
1B. IPCONFIG - Disponível para NT workstation e NT 2000
===

O utilitário no NT para verificar as configurações TCP/IP é um aplicativo que deve ser executando em um prompt do MS-DOS.

O comando IPCONFIG /? Mostrará as opções de parâmetros disponíveis.

TROUBLESHOOTING DE CONECTIVIDADE EM TCP/IP

Configuração de IP do Windows 2000

USO:

ipconfig [/? | /all | /release [adaptador] | /renew [adaptador]

| /flushdns | /registerdns

| /showclassid adaptador

| /setclassid adaptador [id_classe_a_ser_definida]]

adaptador Padrão ou nome completo com '*' e '?' para 'correspondência', * corresponde a qualquer caracter; ? corresponde a um caracter.

Opções:

/? Exibe esta mensagem de ajuda.

/all Exibe as informações completas de configuração.

/release Libera o endereço IP para o adaptador especificado.

/renew Renova o endereço IP para o adaptador especificado.

/flushdns Limpa o DNS Resolver Cache.

/registerdns Atualiza todas as concessões do DHCP e registra novamente os nomes DNS

/displaydns Exibe o conteúdo do DNS Resolver Cache.

/showclassid Exibe todas as identificações de classe do DHCP aceitas para o adaptador.

/setclassid Modifica a identificação de classe do DHCP.

O padrão , a exibição apenas dos endereços IP, da máscara de sub-rede e

do padrão para cada adaptador ligado ao TCP/IP.

No caso de Release e Renew, se não for especificado um nome de adaptador, todas as concessões de endereço IP para todos os adaptadores ligados ao TCP/IP serão liberadas ou renovadas.

Para SetClassID, se não for especificada uma identificação de classe, a identificação de classe ser removida.

Exemplos:

> ipconfig ... Mostra as informações.

> ipconfig /all ... Mostra as informações detalhadas

> ipconfig /renew ... Renova todos os adaptadores

> ipconfig /renew EL* ... Renova adaptadores denominados como EL....

> ipconfig /release *ELINK?21* ... Libera todos os adaptadores correspondentes, por exemplo, ELINK-21, meu_adaptadorELELINKi21.

IPCONFIG sem parâmetros mostra somente o endereço IP , a máscara de rede e o gateway padrão para cada placa de rede associada à estação de trabalho.
IPCONFIG /ALL mostrará informações mais detalhadas tais como o host name da estação, o servidor de DNS, o endereço do adaptador (MAC address) e o servidor de DHCP.

configuração de IP do Windows 2000

Nome do host . . . . : rp33766
Sufixo DNS primário. . . . . . . :
Tipo de nó . . . . : Difusão

Roteamento de IP ativado . . . . . : Não

Proxy WINS ativado . . . . : Não

Lista de pesquisa de sufixo DNS. . : trf3.gov.br

Ethernet adaptador Conexão de rede local:

Sufixo DNS específico de conexão . : trf3.gov.br
Descrição. . . . . : Intel 21041 Based PCI Ethernet Adapter
Endereço físico. . . . . : 00-80-AD-1C-AD-77

DHCP ativado . . . . : Sim

Configuração automática ativada. . : Sim

Endereço IP. . . . . : 10.1.1.202

Máscara de sub-rede. . . . . : 255.255.0.0

Gateway padrão . . . . : 10.1.0.100

Servidor DHCP. . . . . : 10.1.0.21

Servidores DNS . . . . : 10.1.0.12
Concessão obtida . . . . : sexta-feira, 1 de setembro de 2000 08:48:08

Concessão vence em . . . . : quarta-feira, 6 de setembro de 2000 08:48:08

Os parâmetros release e renew são usados para liberar e renovar os endereços que foram obtidos via DHCP. Se houver mais de um adaptador, todos serão acionados, a menos que o adaptador seja especificado.

2. PING

PING é o utilitário básico, disponível no Windows, para verificar conectividade dentro de uma rede e é muito útil para resolver problemas de TCP/IP. O PING envia um pacote ICMP, por default de 32 bytes (configurável), para um host específico e espera que o host responda com os mesmos dados enviados. Se a resposta não vier pode-se assumir que o host esteja down, ou um roteador no meio do caminho esteja down ou a pilha TCP/IP de sua estação de trabalho não esteja funcionando.

Se você receber a resposta, então pode-se assumir que a conectividade entre sua estação e o host analisado esteja operacional.

Para executar o comando PING precisa ser aberto um prompt do DOS ou executar diretamente o comando via INICIAR, EXECUTAR.

Ping novell.com

Pinging www.novell.com [139.15.2.3] with 32 bytes of data:
Reply from 139.15.2.3:bytes=32 time=22ms TTL=59
Reply from 139.15.2.3:bytes=32 time=57ms TTL=59
Reply from 139.15.2.3:bytes=32 time=33ms TTL=59
Reply from 139.15.2.3:bytes=32 time=34ms TTL=59

Pode-se simplesmente entrar com o endereço ip: ping 139.15.2.3 e receber a mesma resposta.
Entretanto se você desconhece o endereço IP de um Host, o ping é uma forma de descobri-lo. Dando o Ping a um nome de DNS faz com que a estação cliente faça uma consulta ao servidor de nomes de domínio antes de enviar o pacote ICMP. Isto também servirá para saber se o seu servidor de domínio está funcionando apropriadamente.
Se falhar o servidor de domínio você receberá mensagem **bad IP address**, ou **host desconhecido** ou **Unable to resolve**, dependendo da versão de seu protocolo TCP/IP.

As possíveis causas de se não resolver o nome são:

- O servidor de nome ou o nome de domínio do DNS não estão configurados apropriadamente na estação de trabalho.
- O servidor DNS para o qual você está apontando não está operacional.

TROUBLESHOOTING DE CONECTIVIDADE EM TCP/IP

O utilitário PING tem muitas opções. Por default, 4 pacotes são enviados (ou 3). Com a opção **–n** (contador) você pode especificar quantidade diferente de pacotes.
Se você tiver problema de intermitência pode-se pingar continuamente com a opção **–t**. Com CRTL-C interrompe-se a execução do comando.

Por default o tamanho do pacote ICMP é de 32 bytes que pode ser alterado com o parâmetro **–l.** Isto pode ser útil para ver se está havendo problema de configuração de tamanho de pacote através dos roteadores da rede.

As opções disponíveis do comando PING são:

Uso: ping [-t] [-a] [-n num] [-l tamanho] [-f] [-i TTL] [-v TOS]

[-r num] [-s num] [[-j lista_hosts] | [-k lista_hosts]]

[-w tempo_limite] lista_destino

Opções:

-t Dispara contra o host especificado até ser interrompido.
Para ver estatísticas e continuar, pressione CTRL-Break;
para terminar, pressione CRTL-C.

-a Resolve endereços para nomes de host.
-n num Número de requisições de eco a enviar.
-l tamanho Envia o tamanho do buffer.
-f Ativa o sinalizador de não-fragmentação no pacote.
-i TTL Define o tempo de vida.
-v TOS Define o tipo de serviço.
-r num Rota dos pacotes para <num> saltos.
-s num Data e hora para <num> saltos.
-j lista_hosts Rota ampliada de origens definida em <lista_hosts>.
-k lista_hosts Rota restrita de origens definida em <lista_hosts>.
-w tempo_limite Tempo limite em milissegundos a aguardar para cada resposta.

NOTAÇÃO DECIMAL DO ENDEREÇO IP

O endereço Ip também pode ser escrito em notação decimal, como um número inteiro.

Por exemplo:

O endereço IP 10.1.1.98 pode ser escrito como 167838050, que pode ser usado no comando PING

Pode-se executar: PING 167838050.

Um dos usos interessantes é para ordenar endereços.

Seja IP p1.p2.p3.p4 – Notação decimal: $p1*256^3 + p2*256^2+p3*256+p4$

3. TRACERT

O comando **TRACERT** tem a finalidade de traçar a rota para um host específico mostrando todos os saltos (hops) que são usados para se chegar ao destino. É um comando muito útil para se identificar áreas da rede com perda de conectividade e problemas de rotas.
O comando TRACERT sem parâmetros mostrará um help com a sintaxe completa disponível:

Uso: tracert [-d] [-h nmax_saltos] [-j lst_hosts] [-w tempo_limite] destino

Opções:

-d Não resolver endereços para nomes de hosts.

-h nmax_saltos Número máximo de saltos para a procura do destino.

-j lst_hosts Rota ampliada de origens usada com a lista lst_hosts.

-w tempo_limite Tempo de espera em milissegundos para cada resposta.

Exemplo:

Ping 10.10.1.1

Rastreando a rota para 10.10.1.1 com no máximo 30 saltos

1 <10 ms 10 ms <10 ms router-ts.trf3.gov.br [10.1.0.100]

2 <10 ms * <10 ms 10.1.0.103

3 30 ms 50 ms 40 ms 132.10.1.1

4 60 ms * 30 ms 10.10.1.1

Rastreamento completo.

4. ARP (ADDRESS RESOLUTION PROTOCOL)

O comando **ARP** permite mostrar e modificar o cache de ARP da estação cliente. O cache de ARP de uma estação cliente é uma tabela de endereços IP e respectivos endereços de adaptador de rede (MAC address). Esta tabela é acessada quando o cliente precisa enviar um pacote de dados para um outro host.
O TC/IP precisa do endereço IP e do endereço do adaptador de destino. O aplicativo que está enviando os dados provê o endereço IP e o TCP/IP precisa conhecer o MAC do destino. Isto é obtido por meio do envio de pacotes de broadcast ARP que solicitam o endereço MAC para um IP específico. A informação é mantida em uma tabela e consultada pela aplicação para reduzir a necessidade de envio de novos pacotes ARP toda vez que um pacote de dados tenha que ser enviado.

Periodicamente é útil consultar esta tabela. Se uma estação cliente não consegue se comunicar com outra estação cliente na rede local , pode-se consultar o cache de ARP (comando ARP –A) para ver se há dados corrompidos ou inválidos. Se a tabela está vazia ou há problemas físicos de conexão ou o host , com o qual está se tentando estabelecer comunicação, não existe. Se existir uma entrada na tabela, certifique-se de que o MAC esteja correto ou se um outro host esteja respondendo em nome do client procurado (roteador, proxy arp, etc.)
Pode-se manualmente apagar e adicionar entradas na tabela ARP.

O comando ARP sem parâmetros trás uma explicação da sintaxe:

```
arp

Exibe e modifica as tabelas de conversão de endereços IP para endereços físicos
usadas pelo
protocolo de resolução de endereços (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

  -a          Exibe entradas ARP atuais interrogando os dados
              de protocolo atuais. Se inet_addr for especificado, somente os e
endereços IP e físicos
              do computador especificado serão exibidos. Se
                                  mais de uma interface de rede usar ARP, serão exibidas as entradas para cada
                                  tabela ARP.
  -g          O mesmo que -a.
  inet_addr   Especifica um endereço Internet.
  -N if_addr  Exibe as entradas ARP para cada interface de rede especificada
              por if_addr.
  -d          Exclui o host especificado por inet_addr. O inet_addr pode ser

              marcado com o caractere * para exclusão de todos os hosts.
  -s          Adiciona o host e associa o endereço Internet inet_addr
              ao endereço físico eth_addr.  O endereço físico é
              passado como 6 bytes hexadecimal separados por hífens. A entrada

              é permanente.
  eth_addr    Especifica um endereço físico.
  if_addr     Caso esteja presente, especifica o endereço Internet da
              interface cuja tabela de conversão de endereços deve ser modificada.
              Caso contrário, é usada a primeira interface aplicável.
Exemplo:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adiciona uma entrada estática
.
  > arp -a                                .... Exibe a tabela ARP.
```

5. NETSTAT

NETSTAT é a ferramenta mais importante para troubleshooting de TCP/IP. Este comando mostra as estatísticas de protocolos e as informações correntes de conexão em TCP/IP para o host onde o comando está sendo executado. A opção **–e** é muito útil. Ela mostra as estatísticas Ethernet, inclusive pacotes descartados e erros de comunicação. Havendo uma suspeita de qualidade de uma placa de rede, este é um comando que

pode ajudar no diagnóstico.

Estatísticas TCP e ICMP oferecem dicas muito úteis para resolver a maioria dos problemas de conexão. A opção **–s** mostra estatísticas IP, ICMP, UDP e TCP.

A opção **–r** ajuda a resolver problemas de rota. Deve sempre existir uma rota default (0.0.0.0) para o roteador local da subrede onde a estação está residente. Se não existir um roteador default, não será possível a comunicação com redes externas.

Há três formas possíveis para criar-se uma rota default:

1. Através do utilitário padrão TCP/IP no ícone REDE do Painel de Controle. Esta informação precisa ser permanente.
2. Informação fornecida automaticamente através de um servidor de DHCP.
3. Adicionando uma rota estática com o comando **route add**. Este comando tem a desvantagem de ter que ser reexecutado toda vez que a estação tiver que ser reiniciada.

A opção –a irá mostrar as conexões TCP ativas , informando o número das portas e os hosts com os quais a estação está se comunicando. O Rastreamento de conexões e a identificação de portas ativas são facilmente executados com este comando.

Para se conhecer todas as opções possíveis do comando NETSTAT:

netstat /?

Exibir estatísticas de protocolo e conexões de rede TCP/IP atuais.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]

-a Exibe todas as conexões e portas de escuta.
-e Exibe estatísticas Ethernet. Isso pode ser combinado à opção -s.
-n Exibe endereços e números de porta em formato numérico.
-p proto Exibe conexões para o protocolo especificado por protocolo.
pode ser TCP ou UDP. Se usado com a opção -s para exibir estatísticas por protocolo, proto pode ser TCP, UDP ou IP.
-r Exibe o conteúdo da tabela de roteamento.
-s Exibe estatísticas por protocolo. Por padrão, as estatísticas são mostradas para TCP, UDP e IP; a opção -p pode ser usada para especificar um subconjunto do padrão.
intervalo Exibe novamente uma estatística selecionada, fazendo pausas de intervalos de segundos entre cada tela. Pressione CTRL+C para interromper a nova exibição das estatísticas. Caso omitido, netstat imprimirá as informações de configuração uma vez.

6. ROUTE

O comando ROUTE server, para, em tempo real, manipular as rotas da estação de trabalho. Pode-se adicionar, alterar, remover e visualizar rotas.

Äs vezes você precisa fazer um acesso a algum equipamento de sua rede, para efeito de monitoração, no entanto seu servidor DHCP não fornece rota para aquele equipamento. Neste, caso utilize o

comando ROUTE ADD para adicionar a rota necessária para permitir o acesso desejado. A desvantagem deste comando é que só vale enquanto seu computador estiver ligado. Após ser reiniciado as configurações serão perdidas. Para tornar rotas alternativas definitivas, o comando deverá ser adicionado no ***autoexec.bat***.

À Sintaxe básica do comando **route** é:

ROUTE [-f] [comando [rede ip destino] [Máscara de sub-rede] [gateway]]

O comando ROUTE sem parâmetros mostra o Help completo.

```
C:\WINDOWS>route

Manipulates network routing tables.

ROUTE [-f] [command [destination] [MASK netmask] [gateway]]

  -f          Clears the routing tables of all gateway entries.  If this is
              used in conjunction with one of the commands, the tables are
              cleared prior to running the command.

  command     Specifies one of four commands
                PRINT     Prints a route
                ADD       Adds a route
                DELETE    Deletes a route
                CHANGE    Modifies an existing route

  destination Specifies the host to send command.

  MASK        If the MASK keyword is present, the next parameter is
              interpreted as the netmask parameter.

  netmask     If provided, specifies a sub-net mask value to be associated
              with this route entry.  If not specified, if defaults to
              255.255.255.255.

  gateway     Specifies gateway.

All symbolic names used for destination or gateway are looked up in the
network and host name database files NETWORKS and HOSTS, respectively.  If
the command is print or delete, wildcards may be used for the destination and
gateway, or the gateway argument may be omitted.
```

OBS: Observe que o comando **ROUTE PRINT** tem a mesma saída do comando **NETSTAT –rn.**

7. NBTSTAT

NBTSTAT é muito útil para identificar informações de uma estação local e remota. O comando utiliza os serviços de NetBios sobre TCP/IP para pode recuperar as informações. A grande vantagem deste comando é a capacidade de recuperar informações de outros segmentos remotos da rede.

Por exemplo, identificando dados de uma estação remota:

nbtstat -A 10.10.10.31

Conexão de rede local:
Endereço-Ip nó: [10.1.1.202] Identificador de escopo: []

Tabela de nomes de máquinas remotas de NetBIOS

Nome	Tipo	Status	
RP50151	<00>	UNIQUE	Registrado
CM_CAMP	<00>	GROUP	Registrado
RP50151	<03>	UNIQUE	Registrado
RP50151	<20>	UNIQUE	Registrado
CM_CAMP	<1E>	GROUP	Registrado
FSUBINAS	<03>	UNIQUE	Registrado
CM_CAMP	<1D>	UNIQUE	Registrado
..__MSBROWSE__.	<01>	GROUP	Registrado

Endereço MAC = 00-50-DA-D7-6F-3C
A estação 10.10.10.31 tem o nome RP50151, pertence ao grupo (ou Domínio) CM_CAMP e está logado, no momento o usuário FSUBINAS. O MAC do adaptador é 00-50-DA-D7-6F-3C.

Para se conhecer todas as opções deste comando, basta digitá-lo sem parâmetros:

NBTSTAT

Exibe as estatísticas de protocolo e as conexões TCP/IP atuais que usam NBT (NetBIOS sobre TCP/IP).

NBTSTAT [-a Nome-remoto] [-A Endereço IP] [-c] [-n]
[-r] [-R] [-s] [S] [intervalo]]

-a (status do adaptador) Lista a tabela de nomes da máquina remota segundo seu nome
-A (Status do adaptador) Lista a tabela de nomes da máquina remota segundo seu endereço IP.
-c (cache) Lista os caches de nome remoto incluindo os endereços IP
-n (nomes) Lista nomes de NetBIOS locais.
-r (resolvido) Lista nomes resolvidos por difusão e através do WINS
-R (Recarregar) Limpa e recarrega a tabela de nomes de caches remotas
-S (Sessões) Lista a tabela de sessões com endereços de IP de destino
-s (sessões) Lista a tabela de sessões que converte endereços IP de destino em nomes NETBIOS de computador.
-RR (ReleaseRefresh) Envia pacotes de liberação de nomes para WINs e inicia a atualização

Nome-remoto Nome remoto da máquina de host.
Endereço IP Representação decimal pontilhada do endereço IP.
intervalo Exibe novamente as estatísticas selecionadas, interrompendo por alguns segundos para intervalo entre cada exibição. Pressione Ctrl+C para interromper a nova exibição estatística.

ROTEIRO PARA VERIFICAÇÃO DE PROBLEMAS DE REDE

TROUBLESHOOTING DE CONECTIVIDADE EM TCP/IP

1. Descubra o endereço IP de sua estação de trabalho e tente dar um PING. Se não obtiver resposta então o TCP/IP de sua máquina não está operando. Pode-se dar PING 127.0.0.1. Este é o endereço de loopback da estação client e é a mesma coisa que dar ping no endereço IP. Rode winipcfg (ou ipconfig) para ver se você obteve endereço de um servidor DHCP ou se a pilha IP está funcionando. Se seu IP for 0.0.0.0 ou um IP de Autoconfiguração pode ser que o servidor de DHCP esteja inoperante ou , se este não for o caso, você pode precisar reinstalar o TCP/IP.

2. Dê um Ping em um endereço IP conhecido de sua rede local. Se falhar há algumas possibilidades a se analisar. O host para o qual você esta enviando o ping pode estar desligado. Pode estar havendo algum problema de rede, como por exemplo, um hub desligado ou defeituoso. Tente um ping de uma outra estação para a sua para certificar-se que seu TCP/IP esteja operacional. Verifique a tabela ARP para ver se há uma entrada para o IP destino.

3. Dê um Ping para um endereço em um outro segmento de rede ou dê um ping nos roteadores do seu segmento de rede. Se falhar e os testes anteriores não, você deve ter problemas de roteamento ou o roteador default está errado. Edite a tabela de roteamento (netstat –rn) para verificar isso. No caso de haver um servidor de DHCP, o roteador default configurado no servidor DHC pode estar configurado errado. Tente dar ping em estações de outras redes quais redes você está alcançando Pode-se, neste caso, usar o tracert com o mesmo objetivo.

4. Verifique a resolução de nomes dentro de sua rede. Dê um Ping em um nome de domínio que esteja na sua rede local. Se falhar, o servidor default de DNS pode ser inválido ou estar desativado.

5. Verifique a resolução de nomes na Intenet. Dê um Ping em um host da Internet (por exemplo: www.cisco.com). Se falhar ou seu DNS externo não está funcionando, ou seu link com a Internet está desativado.